From: SANS AtRisk
To: ndaigle@bakersfieldpd.us
Subject: @RISK: The Consensus Security Vulnerability Alert: Vol. 19, Num. 20
Date: Thursday, May 16, 2019 5:31:18 AM
Attachments: smime.p7s

@RISK: The Consensus Security Vulnerability Alert
May 16, 2019 - Vol. 19, Num. 20

Providing a reliable, weekly summary of newly discovered attack vectors, vulnerabilities with active exploits, and explanations of how recent attacks worked

Archived issues may be found at http://www.sans.org/newsletters/at-risk

---

CONTENTS:

- NOTABLE RECENT SECURITY ISSUES
- INTERESTING NEWS FROM AROUND THE SECURITY COMMUNITY
- VULNERABILITIES FOR WHICH EXPLOITS ARE AVAILABLE
- MOST PREVALENT MALWARE FILES May 9 -16, 2019

TOP VULNERABILITY THIS WEEK: Microsoft releases monthly security update

---

********** **Sponsored By Amazon Web Services, Inc.** **********

AWS Security Operations in the Cloud training series: ***How to Build a Data Protection Strategy in AWS***. In this webcast, SANS instructor Dave Shackleford and AWS solutions architect David Aiken share tips on how to securely migrate data protection policies, processes and tools through the AWS Marketplace. **Tuesday, May 21, 2 PM EDT**.

http://www.sans.org/info/212665

TRAINING UPDATE

SANSFIRE 2019 | Washington, DC | June 15-22

Enterprise Defense Summit & Training 2019 | Redondo Beach, CA | June 3-10

SANS Kansas City 2019 | June 10-15

Security Operations Summit 2019 | New Orleans, LA | June 24-July 1

SANS Charlotte 2019 | July 8-13

SANS Pittsburgh 2019 | July 8-13

SANS Columbia 2019 | Columbia, MD | July 15-20

SANS Rocky Mountain 2019 | Denver, CO | July 15-20

SANS San Francisco Summer 2019 | July 22-27

SANS Cyber Defence Canberra 2019 | June 24-July 13

SANS London July 2019 | July 8-13

SANS OnDemand and vLive Training
Get a Free GIAC Certification Attempt or Take $350 Off your OnDemand or vLive course. Offer ends May 29.

Single Course Training
SANS Mentor and Community SANS

View the full SANS course catalog and skills roadmap

Sponsored Links:

ICYMI: ***Increasing Visibility with Ixia's Vision ONE*** with Serge Borso and Taran Singh. Register: **http://www.sans.org/info/212805**

ICYMI: ***New Year, Same Magecart: The Continuation of Web-based Supply Chain Attacks.*** Get it here: **http://www.sans.org/info/212810**

How is your organization responding to the threats that matter? Take this SANS survey and enter for a chance to win a $400 Amazon gift card: **http://www.sans.org/info/212815**

NOTABLE RECENT SECURITY ISSUES

SELECTED BY THE TALOS SECURITY INTELLIGENCE AND RESEARCH GROUP

Title: **Microsoft patches 79 vulnerabilities, 22 critical**
Description: Microsoft released its monthly security update today, disclosing a variety of vulnerabilities in several of its products. The latest Patch Tuesday covers 79 vulnerabilities, 22 of which are rated "critical," 55 that are considered "important" and one "moderate." This release also includes two critical advisories: one covering Microsoft Live accounts and another addressing updates to Adobe Flash Player. This month's security update covers security issues in a variety of Microsoft's products, including the Scripting Engine, the Microsoft Edge web browser and GDI+.
Reference: **https://blog.talosintelligence.com/2019/05/MS-Patch-Tuesday-May-2019.html**
Snort SIDs: 50068 - 50091, 50115 - 50119, 50120 - 50122

Title: **Adobe fixes critical bugs in Flash Player, Acrobat Reader**
Description: Adobe disclosed 87 vulnerabilities in a variety of its products as part of its monthly security update. The majority of the bugs exist in Adobe Acrobat and Acrobat Reader. There are also critical arbitrary code execution vulnerabilities in Adobe Flash Player and Reader.
Reference: **https://threatpost.com/adobe-flash-acrobat-reader-flaws/144716/**
Snort SIDs: 48293, 48294, 49189, 49190, 49684, 49685

INTERESTING NEWS FROM AROUND THE SECURITY COMMUNITY

WhatsApp is urging users to update the app as soon as possible after it was reported attackers could install malware on a mobile device just by calling the phone through WhatsApp.
https://www.wired.com/story/whatsapp-hack-phone-call-voip-buffer-overflow/

Photo storage app Ever unknowingly uploaded users' photos to their servers to improve the company's facial recognition technology, which it sold to other firms.
https://www.nbcnews.com/tech/security/millions-people-uploaded-photos-ever-app-then-company-used-them-n1003371

Baltimore's city government continues to recover from a ransomware attack. A week later, all of the city's emails, phones and computers are still offline.
https://www.wbaltv.com/article/baltimore-government-is-still-recovering-from-ransomware-attack/27457696

The U.S. Department of Justice charged six people with stealing $2.4 million worth of cryptocurrency over several months in a SIM card hijacking campaign.
https://www.cyberscoop.com/hackers-allegedly-stole-2-4-million-cryptocurrency-six-month-sim-hijacking-spree/

A new bill in Congress would require all U.S. lawmakers to undergo annual cybersecurity and IT training.
https://www.infosecurity-magazine.com/news/lawmakers-propose-cyber-training-1/

A bug in Twitter's iOS app mistakenly shared users' location data with a yet-to-be-named third party.
https://techcrunch.com/2019/05/13/twitter-bug-disclosed-some-users-location-data-to-an-unnamed-partner/

RECENT VULNERABILITIES FOR WHICH EXPLOITS ARE AVAILABLE

COMPILED BY THE QUALYS VULNERABILITY RESEARCH TEAM

This is a list of recent vulnerabilities for which exploits are available. System administrators can use this list to help in prioritization of their remediation activities. The Qualys Vulnerability Research Team compiles this information based on various exploit frameworks, exploit databases, exploit kits and monitoring of internet activity.

ID: CVE-2019-1862
Title: **Cisco IOS XE Software Web UI Command Injection Vulnerability**
Vendor: Cisco
Description: A vulnerability in the web-based user interface of Cisco IOS XE Software could allow an authenticated, remote attacker to execute commands on the underlying Linux shell of an affected device with root privileges.
CVSS v2 Base Score: 9.0 (AV:N/AC:L/Au:S/C:C/I:C/A:C)

ID: CVE-2019-1649
Title: **Cisco Secure Boot Hardware Tampering Vulnerability**
Vendor: Cisco
Description: A vulnerability in the logic that handles access control to one of the hardware components in Cisco's proprietary Secure Boot implementation could allow an authenticated, local attacker to write a modified firmware image to the component. This vulnerability affects multiple Cisco products that support hardware-based Secure Boot functionality.
CVSS v2 Base Score: 6.2 (AV:L/AC:M/Au:S/C:P/I:C/A:C)

ID: CVE-2019-5018
Title: **SQLite Use After Free Remote Code Execution Vulnerability**
Vendor: SQLite
Description: SQLite is exposed to remote code execution vulnerability. Successfully exploiting this issue allows attackers to execute arbitrary code in the context of the affected application.
An exploitable use after free vulnerability exists in the window function functionality of Sqlite3. A specially crafted SQL command can cause a use after free vulnerability, potentially resulting in remote code execution. An attacker can send a malicious SQL command to trigger this vulnerability.
CVSS v2 Base Score: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

ID: CVE-2019-5021
Title: **Alpine Linux Docker Image Hard Coded Credentials Authentication Bypass Vulnerability**
Vendor: Alpine Linux
Description: Alpine Linux Docker Image is exposed to an authentication-bypass vulnerability. An attacker can exploit this issue to gain unauthorized access or obtain sensitive information; this may lead to further attacks. Due to the nature of this issue, systems deployed using affected versions of the Alpine Linux container which utilize Linux PAM, or some other mechanism which uses the system shadow file as an authentication database, may accept a NULL password for the `root` user.
CVSS v2 Base Score: 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

ID: CVE-2019-3400
Title: **Atlassian JIRA Cross Site Scripting Vulnerability**
Vendor: Atlassian
Description: Atlassian JIRA is exposed to a cross site scripting vulnerability because it fails to properly sanitize user supplied input. An attacker may leverage this issue to execute arbitrary HTML and script code in the browser of an unsuspecting user in the context of the affected site. This may let the attacker steal cookie based authentication credentials and launch other attacks. It allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting vulnerability in the jql parameter.
CVSS v2 Base Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

ID: CVE-2019-2725
Title: **Oracle WebLogic Server Deserialization Remote Command Execution Vulnerability**
Vendor: Oracle
Description: Oracle WebLogic Server is exposed to a remote command execution vulnerability. Attackers can exploit this issue to execute an arbitrary command within the context of a user running the affected application. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server.
CVSS v2 Base Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

ID: CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091
Title: **Intel Processor MDS Vulnerabilities**
Vendor: Intel
Description: Modern Intel microprocessors implement hardware level micro optimizations to improve the performance of writing data back to CPU caches. These vulnerabilities are collectively referred as Microarchitectural Data Sampling issues (MDS issues) because they refer to issues related to microarchitectural structures of the Intel processors other than the level 1 data cache. The affected microarchitectural structures in the affected Intel processors are the Data Sampling Uncacheable Memory (uncacheable memory on some microprocessors utilizing speculative execution), the store buffers (temporary buffers to hold store addresses and data), the fill buffers (temporary buffers between CPU caches), and the load ports (temporary buffers used when loading data into registers). As a result of the flaw in the architecture of these processors, an attacker who can execute malicious code locally on an affected system can compromise the confidentiality of data previously handled on the same thread or compromise the confidentiality of data from other hyperthreads on the

same processor as the thread where the malicious code executes.
CVSS v2 Base Score: 4.9 (AV:L/AC:L/Au:N/C:C/I:N/A:N)

MOST PREVALENT MALWARE FILES May 9 - 16, 2019
COMPILED BY TALOS SECURITY INTELLIGENCE AND RESEARCH GROUP

SHA 256: e4cef790c953b769c08472ace6d6f3321851fb701882ebcb76a78a413ed85505
MD5: 2c5d83f7abe17e9ccdd6dcc0622a22aa
VirusTotal:
https://www.virustotal.com/#/file/e4cef790c953b769c08472ace6d6f3321851fb701882ebcb76a78a413ed85505/details
Typical Filename: $RECYCLE.BIN .scr
Claimed Product: N/A
Detection Name: Win.Worm.Sality::1201

SHA 256: 3f6e3d8741da950451668c8333a4958330e96245be1d592fcaa485f4ee4eadb3
MD5: 47b97de62ae8b2b927542aa5d7f3c858
VirusTotal:
https://www.virustotal.com/#/file/3f6e3d8741da950451668c8333a4958330e96245be1d592fcaa485f4ee4eadb3/details
Typical Filename: qmreportupload.exe
Claimed Product: qmreportupload
Detection Name: Win.Trojan.Generic::in10.talos

SHA 256: 2c8cb61f622f8c4c4babc19ebf9fad759d9913c4ca47ad393448c48bad08d71a
MD5: 3a61797cff12598b31443d5bce21e470
VirusTotal:
https://www.virustotal.com/#/file/2c8cb61f622f8c4c4babc19ebf9fad759d9913c4ca47ad393448c48bad08d71a/details
Typical Filename: WcInstaller.exe
Claimed Product: Web Companion Installer
Detection Name: W32.2C8CB61F62-95.SBX.TG

SHA 256: 7acf71afa895df5358b0ede2d71128634bfbbc0e2d9deccff5c5eaa25e6f5510
MD5: 4a50780ddb3db16ebab57b0ca42da0fb
VirusTotal:
https://www.virustotal.com/#/file/7acf71afa895df5358b0ede2d71128634bfbbc0e2d9deccff5c5eaa25e6f5510/details
Typical Filename: xme64-2141.exe
Claimed Product: N/A
Detection Name: W32.7ACF71AFA8-95.SBX.TG

SHA 256: c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f
MD5: e2ea315d9a83e7577053f52c974f6a5a
VirusTotal:
https://www.virustotal.com/#/file/c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f/details
Typical Filename: Tempmf582901854.exe
Claimed Product: N/A
Detection Name: W32.AgentWDCR:Gen.21gn.1201

SHA 256: 15716598f456637a3be3d6c5ac91266142266a9910f6f3f85cfd193ec1d6ed8b
MD5: 799b30f47060ca05d80ece53866e01cc
VirusTotal:
https://www.virustotal.com/#/file/15716598f456637a3be3d6c5ac91266142266a9910f6f3f85cfd193ec1d6ed8b/details
Typical Filename: 15716598f456637a3be3d6c5ac91266142266a9910f6f3f85cfd193ec1d6ed8b.bin
Claimed Product: N/A
Detection Name: W32.Generic:Gen.22fz.1201

(c) 2019. All rights reserved. The information contained in this newsletter, including any external links, is provided "AS IS," with no express or implied warranty, for informational purposes only.

Please feel free to share this with interested parties via email, but no posting is allowed on web sites. For a free subscription visit https://www.sans.org/account/create

SANS Institute Privacy Policy
11200 Rockville Pike, Suite 200, North Bethesda, MD, 20852

To change your email address visit update profile.

To change your email preferences or unsubscribe visit manage subscriptions.

This mailbox is not monitored. Please email support@sans.org or call 301-654-7267 for assistance.